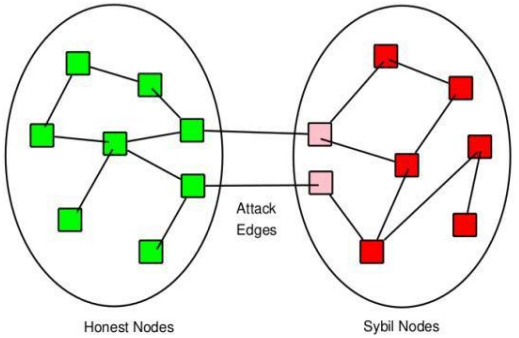
La Toile de Confiance Duniter

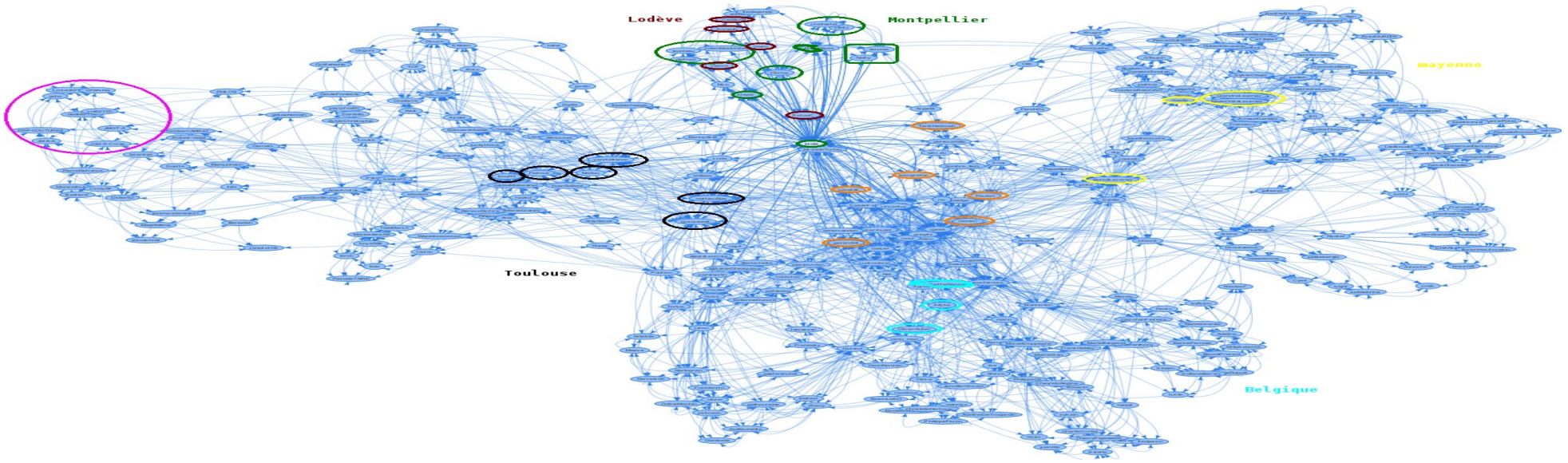
- Intro
- Les 8 règles de la Toile de Confiance
- Les 7 types d'actes en blockchain
- Les 4 types de documents soumis par les clients
- Stockage de la wot
- La wot dans le code du cœur

Auteur :
Éloïs / elois@ifee.fr
https://librelois.fr

Pourquoi une Toile de Confiance ?

Les rôles de la wot (**W**eb **O**f **T**rust) :
1. S'assurer que chaque humain créer un seul DU
2. Identifier les calculateurs pour pouvoir leur attribuer une difficulté personnalisée





Auteur :
Éloïs / elois@ifee.fr
https://librelois.fr

Définition d'une wot Duniter

- Les toiles de confiance duniter (une par monnaie) sont des graphes simples **orientés** et sans sommets isolés.
- Les sommets en sont les membres et les arcs les certifications.
- tout les sommets sont des identités membres ou ayant déjà été membres par le passé, les sommets correspondant aux anciens membres sont dans un état particulier dit "désactivé". (jusqu’à révocation implicite).
- Toute certification reste valide jusqu’à sa date d'expiration dans le but d'éviter un effondrement de la toile en cascade.

Auteur :
Éloïs / elois@ifee.fr
https://librelois.fr

Les 8 règles d'une wot Duniter

1. Règle de distance (stepMax, xPercent)
2. Règle du nombre minimal de certifications reçus (sigQty)
3. Règle de renouvellement (msValidity, msPeriod, msWindow)
4. Règle d'expiration des certifications (sigValidity)
5. Règle du stock limité de certifications **actives** (sigStock)
6. Règle de l'intervalle d'écriture entre deux certifications (sigPeriod)
7. Règle de la fenêtre d'écriture d'une certification (sigWindow)
8. Règle de la fenêtre d'écriture d'une identité (idtyWindow)

Le cas particulier de la wot Initiale

- L'application des 8 règles ne rend l'expansion d'une toile possible qu'a partir d'une toile pré-éxistante, il y a donc un cas particulier ou certaines règles ne s'appliquent pas : l'écriture du block zéro.
- Seules les règles 2 et 5 s'appliquent lors de l'écriture du block zéro. (sigQty et sigStock)
- C'est l'humain qui génère le bloc zéro qui choisi manuellement qu'elles identités il écrira dans le bloc zéro, mais toutes les identités et certifications écrites dans le bloc zéro doivent respecter les règles 2 et 5 et de plus le bloc zéro doit être signé avec la clé privée d'une des identités écrites.
- Dés lors qu'un bloc zéro correct a été généré, toute identité inscrite dans ce bloc zéro peut soumettre le bloc suivant, de fait l'auteur du bloc zéro n'a donc plus la main.

Les 7 types d'actes en blockchain

1. identities (↔ doc Identity)
   PUBKEY:SIGN:I_BLOCK_UID:USER_ID
2. joiners (↔ doc Membership IN)
   PUBKEY:SIGN:M_BLOCK_UID:I_BLOCK_UID:USER_ID
3. actives (↔ doc Membership IN)
   PUBKEY:SIGN:M_BLOCK_UID:I_BLOCK_UID:USER_ID
4. leavers (↔ doc Membership OUT)
   PUBKEY:SIGN:M_BLOCK_UID:I_BLOCK_UID:USER_ID
5. revoked (↔ doc Revocation)
   PUBKEY:SIGN
6. excluded (expiration de membership + descente sous sigQty cert + révocations implicites + révocations explicites)
   PUBKEY
7. certifications (↔ doc Certification)
   PUBKEY_FROM:PUBKEY_TO:BLOCK_ID:SIGN

Les 4 types de documents soumis par les clients

- **Identity**

Version : 10

Type: Identity

Currency: CURRENCY_NAME

Issuer: PUBLIC_KEY

UniqueID: USER_ID

Timestamp: BLOCK_UID

SIGNATURE

- **Membership**

Version: 10

Type: Membership

Currency: CURRENCY_NAME

Issuer: ISSUER

Block: M_BLOCK_UID (*Timestamp)

Membership: MEMBERSHIP_TYPE

UserID: USER_ID

CertTS: BLOCK_UID *(Identity's block UID)

MEMBERSHIP_SIGNATURE

- **Certification**

Version: 10
Type: Certification

Currency: CURRENCY_NAME

Issuer: PUBLIC_KEY

IdtyIssuer: IDTY_ISSUER

IdtyUniqueID: USER_ID

IdtyTimestamp: BLOCK_UID

(IdtySignature: IDTY_SIGNATURE > anti-spam)

CertTimestamp: BLOCK_UID

CERTIFIER_SIGNATURE

- **Revocation**

Version : 10

Type: Revocation

Currency: CURRENCY_NAME

Issuer: PUBLIC_KEY

IdtyUniqueID: USER_ID

IdtyTimestamp: BLOCK_UID

(IdtySignature: IDTY_SIGNATURE)

REVOCATION_SIGNATURE

Stockage de la WoT

- **Wot.bin (module wotb)**

Liste de liens :

1 → 4

2 → 4

3 → 1

4 → 2

…

Chaque membre est représenté par son wotb_id (nombre entier positif)

- **BDD SQLite**
  - Tables blockchain
    - i_index,
    - m_index,
    - c_index
  - Piscines (sandboxs)
    - Idty
    - Membership
    - cert

La WoT dans le code

- Génération du prochain bloc à calculer
  - App/modules/prover/lib/BlockGenerator.ts
- Vérifier la conformité d'un bloc soumis
  - App/lib/blockchain/DuniterBlockchain.ts
    - → checkBlock()
- Indexation d'un bloc empilé
  - App/lib/blockchain/Duniterblockchain.ts
    - → pushTheBlock()

La Toile de Confiance Duniter

Merci pour votre attention !

Auteur :
Éloïs / elois@ifee.fr
https://librelois.fr